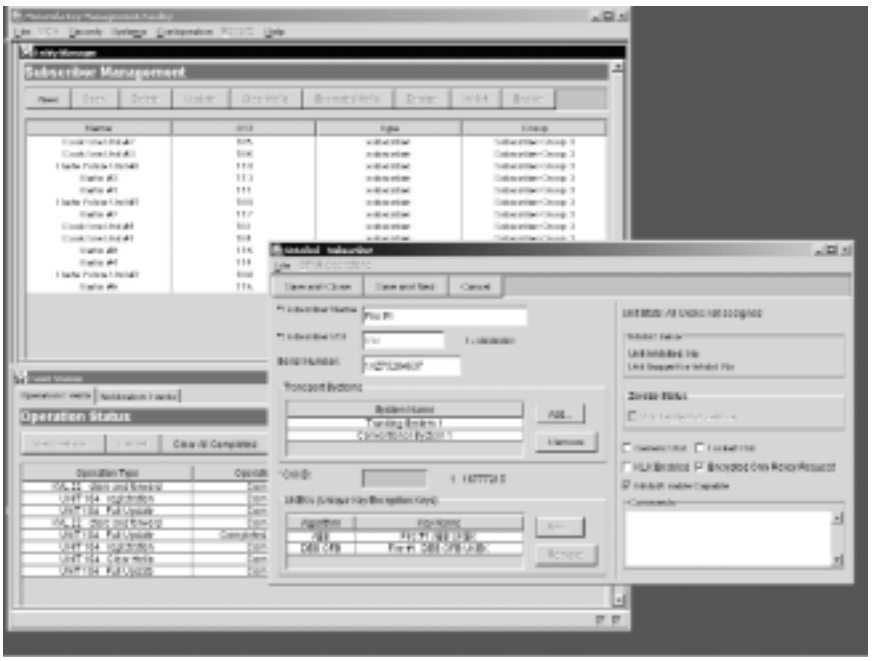
Specification Sheet

KMF (Trunking) Key Management Facility

MOTOROLA
intelligence everywhere™



The Key Management Facility (KMF) is a Project 25 compliant mission critical enterprise solution, which facilitates secure key management and distribution.

INTRODUCTION

The Key Management Facility (KMF) is a Project 25 compliant mission critical enterprise solution, which facilitates secure key management and distribution. The KMF enables effective planning, implementation, and execution of security doctrine for a diverse set of user requirements. The KMF Operator gathers communication requirements into three categories: User Groups, Units, and Common Key References to organize the system effectively. Key assignments are then distributed to each of these categories enabling the Operator to easily distribute and change desired keys. This re-key transaction is performed either via Over-the-Air Rekeying, or via Store & Forward functionality in conjunction with a KVL 3000 Plus. Over-The-Air Control (OTAC) features that exist within the KMF allow the KMF Operator to Inhibit and Enable radios within the network. Event logging, archiving and reporting are additional security features of the KMF.

The KMF is comprised of three system elements: (1) A Client/Server software application; (2) A Windows 2000 Computer Network; and (3) A KMF Crypto Card (CC).

KMF SYSTEM ELEMENTS

(1) KMF Extensions enables Key Management and Over-The-Air Rekeying Services in conjunction with an ASTRO®25 Integrated Voice and Data (IV&D) system. The KMF provides a logical, user friendly interface facilitating highly efficient and secure radio fleet management and rekeying.

(2) The Windows 2000 architecture makes use of commercially available computer platforms running the KMF software application.

(3) The KMF CC is a PCI device that performs encryption and decryption for the KMF's software application.

FEATURES/SERVICES

OVER-THE-AIR REKEYING (OTAR)

Eliminate the burden of manually rekeying your radios on a regular basis. OTAR is a powerful suite of operations that enables key distribution and key management to be conducted securely over-the-air. OTAR solves the logistical problem of maintaining secure wireless communications.

STORE & FORWARD

The KMF exhibits "Store & Forward" operations of the KVL 3000 Plus. During the rekeying operation, associations between units and the KVL 3000 Plus can be performed directly from the user interface. "Store & Forward" permits a user to reach those units that may be out of range and enables an operator to become more efficient with managing their system. The KVL 3000 Plus is capable of directly transmitting rekey messages originated within the KMF server database to a radio or secure capable infrastructure. Each unit's response is securely stored inside the KVL 3000 Plus and then forwarded directly back to the KMF server. The KMF user interface visibly shows an operator which units successfully acknowledged the re-key message for easy key management.

SECURE USER GROUP MANAGEMENT

The KMF provides an innovative concept for managing secure radio communications among user groups, known as Common Key Reference (CKR). Has your organization ever needed to speak securely within and amongst additional groups? Through the CKR concept, an operator is able to visually track the members and encryption keys assigned to each CKR group. In a single CKR update operation, a new key to all members of the group can be sent via OTAR.

RADIO AND GROUP KEY CURRENCY

Have you ever initiated the re-keying process and wondered which radios have been successfully completed? The KMF offers a "Currency" management feature that allows an operator to see exactly which radios are ready for communication.

RETRY OPPORTUNITIES

The KMF offers automated retries of rekey messages when an operator initiates key updates.

REMOTE INHIBIT/ENABLE

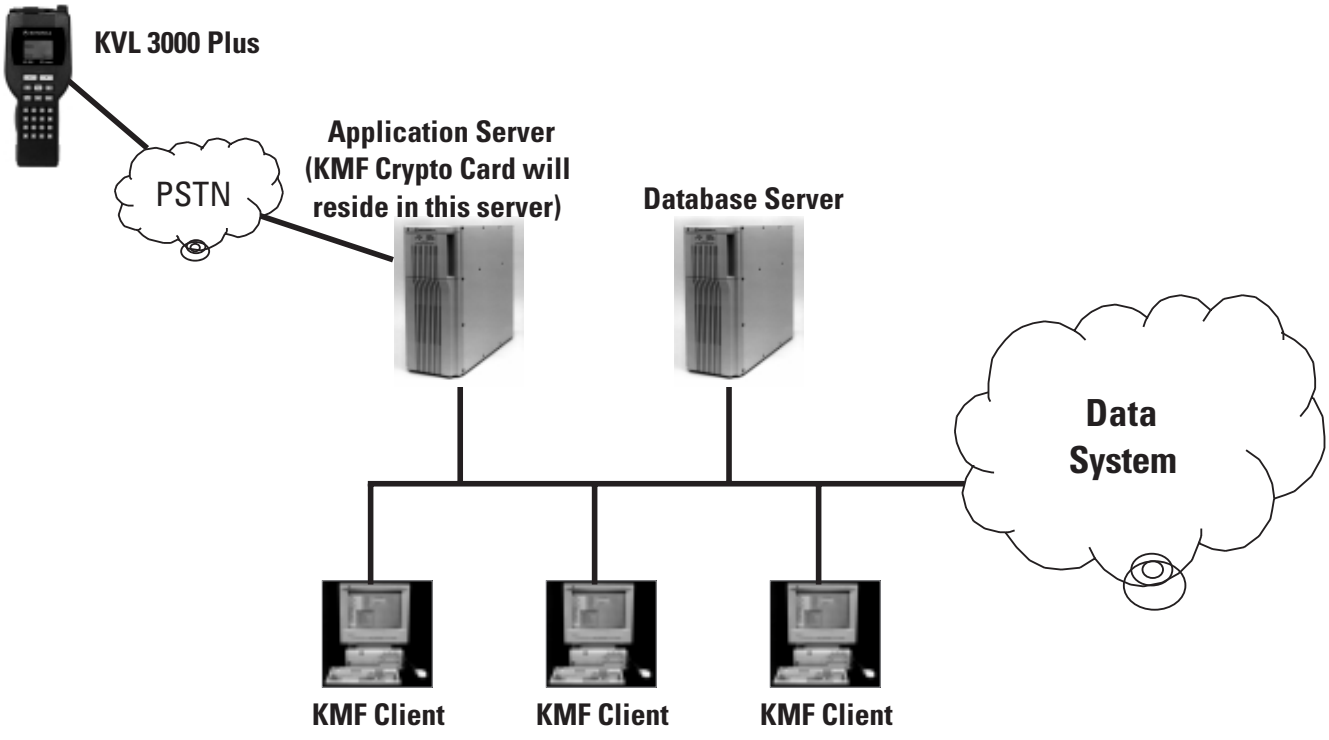
Has a radio been compromised? Securely inhibit a compromised radio over-the-air and protect the integrity of your network. When the radio is recovered, remotely enable the radio and securely re-join your network.

KEY MATERIAL GENERATION

KMF includes a certified key material generator, freeing operators from reliance on third party suppliers or manual key material generation. The operator can simply instruct the KMF to replenish the store of keys when the inventory drops below the necessary volume.

KMF HELLO

Not sure if a radio is within reach of your system network? KMF Hello is a quick and efficient method of determining whether a radio is within range of the system network without introducing unnecessary voice traffic.



KMF System Configuration

KMF SPECIFICATIONS

PROJECT 25 COMPLIANT FEATURES

Add, Modify, Delete Keys

Zeroize

Change-Over

Rekey

Hello

Warm Start

AES and DES-OFB Encryption Algorithm

MOTOROLA SPECIFIC FEATURES

KLK (Key Loss Key) Rekeying

Remote Inhibit/Enable

Multiple Encryption Algorithms Supported: DES-XL, DVI-XL, DVP-XL

PERFORMANCE / CAPACITY

Up to 10 Clients are supported per KMF Server

64,000 unit database capacity (for Trunking systems)

KMF CRYPTO CARD (CC) SPECIFICATIONS

ENCRYPTION ALGORITHMS

AES, DES-OFB, DES-XL, DVI-XL, DVP-XL

POWER

PCI Card	6 Watts maximum
Battery Life	5 Years in powered KMF CC 2 Years in unpowered KMF CC

ENVIRONMENT

Temperature	0 to +50°C
Humidity	20-80%

PERFORMANCE

Key Storage Capacity	1 Master Key per algorithm

PHYSICAL DIMENSIONS

PCI Card	22mm x 127mm x 180mm (H x W x L)
Weight	220 g

CERTIFICATION

FIPS-140-2 Level 1 Security Guidelines

FCC CFR 47, Part 15 subpart B for class B equipment

CE Certification	EN55022: 1998 EN55024: 1998

MINIMUM CLIENT/SERVER REQUIREMENTS

KMF Application Server	KMF Database Server	KMF Client Workstation
ServerWorks GC LE Chipset	ServerWorks GC LE Chipset	Intel 845E Chipset
512 KB cache	512 KB cache	512 KB cache
1 GB RAM	1 GB RAM	512 MB RAM
DVD-RW Drive	DVD-RW Drive	48x CD-ROM
2 Hot Plug 18.2 GB U320 Universal 1"	4 Hot Plug 18.2 GB U320 Universal 1"	40 GB Ultra ATA/100 hard drive (7200 rpm)
RAID Array Controller Card. Required RAID Level (0+1) for drive Array i.e. Drive Array 1 = C:\ (System drive)	RAID Array Controller Card. Required RAID Level (0+1) for both drive Arrays i.e. Drive Array 1 = C:\ (System drive) Drive Array 2 = D:\ (Data drive)	Integrated Ultra ATA/100 IDE Controller
Microsoft Windows 2000 Server with SP4	Microsoft Windows 2000 Server with SP4	Microsoft Windows XP Professional with SP 1a
Integrated Gbit (10/100/1000Mb) Ethernet adapter	Integrated Gbit (10/100/1000Mb) Ethernet adapter	Integrated Gbit (10/100/1000Mb) Ethernet adapter
15" SVGA monitor	15" SVGA monitor	19" SVGA monitor
Integrated Video Controller with 8MB SDRAM Video Memory	Integrated Video Controller with 8MB SDRAM Video Memory	64 MB, Dual Display, AGP Graphic Card
		Capable of running with other Windows XP applications

Malcolm Baldrige National Quality Award 2002 Award Recipient

Motorola's Commercial, Government and Industrial Solutions Sector is a recipient of the prestigious 2002 Malcolm Baldrige National Quality Award. This honor demonstrates our commitment to performance excellence and quality achievement.

MOTOROLA

MOTOROLA and the Stylized M Logo are registered in the U.S. Patent and Trademark Office. All other product or service names are the property of their respective owners.
©Motorola, Inc. 2003. (0309) VPS

Specifications subject to change without notice.

R3-17-2003